(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 August 2003 (07.08.2003)

PCT

(10) International Publication Number
WO 03/065676 A1

(51) International Patent Classification[7]: H04L 29/06, G06F 1/00

(21) International Application Number: PCT/CH02/00050

(22) International Filing Date: 28 January 2002 (28.01.2002)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **PHILIP MORRIS PRODUCTS S.A.** [CH/CH]; Quai Jeanrenaud 3, CH-2000 Neuchâtel (CH).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **PREMAT, Daisy** [CH/CH]; Chemin de Montelly 31, CH-1007 Lausanne (CH). **LEPEZENNEC, Hervé** [FR/CH]; Rue du Cimetière, CH-1328 Mont-la-Ville (CH).

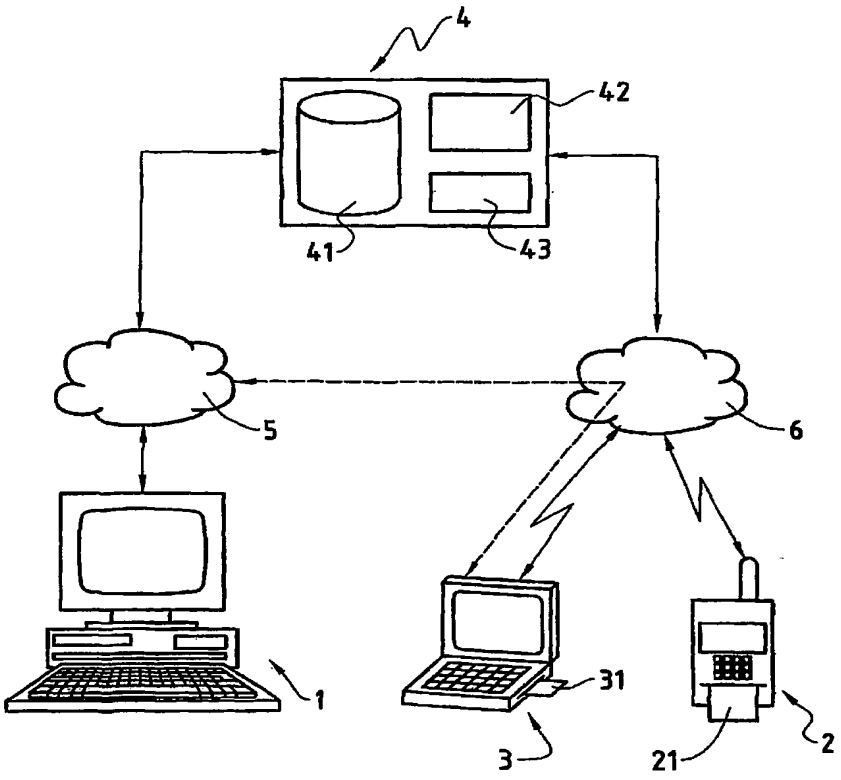
(74) Agent: **BOVARD LTD.**; Optingenstrasse 16, CH-3000 Berne 25 (CH).

(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK (utility model), SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND AUTHENTICATION SERVER FOR CONTROLLING ACCESS TO A RESOURCE ACCESSIBLE THROUGH A COMMUNICATIONS NETWORK



(57) Abstract: Proposed is a method and authentication server (4) for controlling access of a user to a resource accessible through a first communications network (5) by means of a first communication terminal (1, 3). An address (72) of a second communication terminal (2, 3) is stored at the authentication server (4) as part of personal user information (7). The authentication server (4) transmits a challenge code over a second communications network (6) to the second communication terminal (2, 3) identified by said address (72). The challenge code received by the second communication terminal (2, 3) is transmitted by the first communication terminal (1, 3) over the first communications network (5) to the authentication server (4). The authentication server (4) compares the challenge code received from the first communication terminal (1, 3) to the challenge code transmitted to the second communication terminal (2, 3), and the authentication server (4) grants the user access to the resource after having validated the challenge code received from the first communication terminal (1, 3).

WO 03/065676 A1

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv)) for US only*

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Method and Authentication Server for Controlling Access to a Resource Accessible Through a Communications Network

SPECIFICATION

Technical Field

The present invention relates to a method and an authentication server for controlling access to a resource accessible through a communications network. Specifically, the present invention relates to a method and an authentication server for controlling access of a user to a resource accessible through a communications network, for example the Internet, whereby user identification information entered by the user on a communication terminal is transmitted over the communications network to the computerised authentication server and compared to user identification information stored in the database of the authentication server.

Background Art

Typically, controlling access to hardware or software resources available in a communications network requires some form of user identification. The resources are accessed by the users through the communications network by means of communication terminals such as personal computers, personal data organizers or mobile radio telephones. Examples of software resources accessible through communications networks include software programs, software directories, databases and web pages. Before getting granted access to a controlled resource, the user is requested to enter user identification information on his communication terminal. The user identification information entered by the user is transmitted over the communications network to a computerised server, for example an access control server or an authentication server. The server compares the received

user identification information to user identification information stored in a database of the server and grants the user access to the resource, if the received user identification information is validated, i.e. if the received user identification information corresponds to the stored user identification information. The user identification information comprises, for instance, a user name or log-in name and a secret user password or log-in password. In order to prevent eavesdropping of the user identification information, at least the secret password is typically transmitted over the communications network in encrypted form.

To reduce the risk of granting access to a resource to an unauthorised user, who has discovered a secret user password through trial and error, or who has been given a secret user password by an authorised user, for example, an additional level of security has been added for controlling access over a communications network to resources such as banking services. The user is given a personal list with secret codes. With every access to the controlled resource, in addition to the user identification information, the user is requested to enter the secret code on top of the list on his communication terminal and subsequently delete that secret code from the list. Even an unauthorised user who knows the secret password cannot access the resource without access to this list. Nevertheless, users, particularly mobile users, find the use of such lists not very convenient. On one hand, resources cannot be accessed without having the list ready at hand. On the other hand, keeping the list on one's person increases the risk of losing the list or having it stolen. Furthermore, the personal code lists can become a real nuisance to users who have made an error in deleting a secret code from the list, be it that they forgot to delete a code, or be it that they deleted more than one code. Maintaining the list means additional overhead for the users as well as for the resource or service provider. Providers need to ensure that the users are supplied with new lists, whenever the secret codes on a list have all been used.

Disclosure of Invention

It is an object of this invention to propose a new and improved method and authentication server for controlling access to a resource accessible through a communications network, whereby the new method and authentication server at least do not have some of the disadvantages of the prior art.

According to the present invention, these objects are achieved particularly through the features of the independent claims. In addition, further advantageous embodiments follow from the dependent claims and the description.

According to the present invention, these objects are particularly achieved in that for a user, who attempts to access a resource accessible through a first communications network by means of a first communication terminal, an address of a second communication terminal is stored at an authentication server and the authentication server transmits a challenge code over a second communications network to the second communication terminal identified by said address. According to the present invention, the challenge code received by the second communication terminal is transmitted (returned) by the first communication terminal over the first communications network to the authentication server, the authentication server compares the challenge code received from the first communication terminal to the challenge code transmitted to the second communication terminal, and the authentication server grants the user access to the resource after having validated the challenge code received from the first communication terminal.

This approach for controlling access to a resource accessible through a communications network has the advantage that an additional layer of security and control is added to the verification of submitted user identification information, including a user name and password, for example, without adding the overhead required for maintaining personal lists of secret codes. An unauthorised user, who knows the user identification information of an authorised user, cannot get access to the controlled resource, unless, at the

time of access, he is also in possession of the authorised user's second communication terminal or of the authorised user's subscriber identification module (SIM) linking said address to the second communication terminal, respectively. Without possession of the second communication terminal or the SIM, respectively, at the time of access, the unauthorised user cannot receive the challenge code from the authentication server and is, therefore, in no position to return the challenge code to the authentication server. Access to the resource can thus be controlled by checking the knowledge of information, namely the user identification information, and by checking the presence of a pre-defined physical device, namely the personal communication terminal or the SIM, respectively, of the authorised user who is identified by the user identification information. The possession of a specific pre-defined physical device at the time of access as a prerequisite for being granted access to a resource is more stringent than a personal code list because, unlike such a list, the physical device, i.e. the communication terminal or the SIM, cannot be easily copied and shared. Moreover, the security is increased because different communications networks are used to transmit the secret challenge code.

In an embodiment of the present invention, a timer is started by the authentication server after the challenge code has been transmitted to the second communication terminal, and the user is denied access to the resource, if the challenge code is not received from the first communication terminal within a pre-defined time period. Through specification of a time-limit for returning the challenge code to the authentication server, it is possible to reduce the risk that an authorised user receiving the challenge code on his communication terminal communicates the received challenge code to an unauthorised user in a different location, who is using the user identification information of the authorised user.

In an embodiment of the present invention the personal user information is linked to a serial number, the serial number identifying a specific resource, and the user is requested to enter the serial number on the first communication terminal prior to the entry of the user identification information. Linking the personal user information to a serial number identifying a resource

has the advantage that access of a user can be controlled for one or more specific resources.

In an embodiment of the present invention the resources are computer software objects such as computer programs, e.g. computer games, computer databases, computer data, computer directories or web pages, located on the Internet, for example on the worldwide web; the second communication terminal is a mobile communication terminal, for example a mobile radio telephone, whereby the phone number assigned to the mobile communication terminal is used as the address; the challenge code is generated by means of a random generator; and the challenge code is transmitted by the authentication server over a mobile radio network to the mobile communication terminal by means of data messages such as SMS (Short Message Services) or USSD messages (Unstructured Supplementary Services Data). The first communication terminal is for example a personal computer equipped for communication over the Internet; however, the first communication terminal can also be a mobile communication terminal, for example a personal data assistant or a mobile radio telephone, equipped to access both the Internet and the mobile radio network, so that the first communication terminal and the second communication terminal are one and the same physical device.

In addition to the method and authentication server for controlling access to a resource accessible through a communications network, the present invention also relates to a computer program product comprising computer program code to direct a computerised server to execute the functions of the authentication server and to a computer-readable data carrier, encoded with data representing a computer program, that makes it possible to direct a computerised server to execute the functions of the authentication server.

Brief Description of Drawings

The present invention will be explained in more detail, by way of example, with reference to the drawings in which:

Figure 1 is a block diagram illustrating an authentication server connected to two communications networks, communication terminals being connected to the communications networks.

Figure 2 is a block diagram illustrating personal user information linked to a serial number, the personal user information comprising user identification information and an address of a communication terminal.

Figure 3 is a timing diagram illustrating the information exchange between a user, a point of presence, the authentication server and the communication terminals.

Mode(s) for Carrying Out the Invention

In Figure 1, the reference numeral 4 refers to an authentication server which comprises at least one computer with at least one processor 43, a database 41, and a computer-readable data carrier 42. The computer-readable data carrier 42 is encoded with data representing a computer program, that makes it possible to direct the computerised authentication server, respectively its processor(s), to execute the steps S1, S2, S3, S4, and S5, and to initiate the steps A1, A2, A3 and A4, as will be described below. The authentication server 4 can comprise an additional computer to run the database 41.

As is schematically illustrated in Figure 1, the authentication server 4 is connected to two communications networks 5 and 6. The communications network 5 is, for example, the Internet comprising the worldwide web. The

communications network 6 is, preferably, a mobile communications network, for example, a mobile radio network, e.g. a GSM (Global System for Mobile Communications) or a UMTS network (Universal Mobile Telephone System) or another terrestrial or satellite-based mobile radio system. If fixed communications terminals 2 or 3 are used, the communications network 6 could also be a fixed communications terminal, for example the public switched telephone network (PSTN) or an ISDN-network (Integrated Services Digital Network). The function of the authentication server 4 is to control access of a user to a resource accessible through the communications network 5. The resource can be a computer hardware device or a computer software object, for example a computer program, a computer database, computer data, a computer directory or a web page. The resource can be located on a computer of the authentication server 4 or on a computer connected to the authentication server 4.

In Figure 1, examples of the user's communication terminals 1, 2 and 3 are illustrated. The communication terminal 1, for example a personal computer, is connected to the communications network 5, and is equipped to exchange data with the authentication server 4 over the communications network 5. The communication terminal 2 is a mobile communication terminal, for example a radio telephone, and is connected to the communications network 6, and is equipped to exchange data with the authentication server 4 over the communications network 6. The communication terminal 3, for example a personal data organiser with a mobile radio telephone module, is connected to the communications networks 5 and 6, and is equipped to exchange data with the authentication server 4 over the communications networks 5 and 6. Thereby the communications network 5 may be accessed by the communication terminal 3 through the communications network 6, for example using additional means such as WAP (Wireless Application Protocol) and corresponding gateways. The communication terminals 2 and 3 are preferably personal communication terminals, each provided with a subscriber identification module (SIM) 21 or 31, respectively, for example a SIM in the form of a chipcard. A SIM contains a unique user identification, for example an International Mobile Subscriber Identity (IMSI). Conventionally, in a database of the communications network 6, for example in the Home Location Register

(HLR), the user identification stored on the SIM is linked to the address (or phone number) of the communication terminal 1 or 3, respectively.

With reference to Figure 3, the information exchange between the user 9, a point of presence 10, the authentication server 4 and the user's communication terminals 1, 2, and 3 will be explained in the following paragraphs.

At a point of presence 10, for example a shop or a merchandising stand, the user 9 personally communicates in step U1 personal information such as name, mailing address and the address, e.g. the phone number, of his personal communication terminal 2 or 3, to a representative at the point of presence 10, after having provided proof of identity and proof of age by means of official documents such as a driver's license, a passport or another picture identification.

In step P1, the personal information provided by the user is communicated to the database 41 of the authentication server 4 together with a serial number identifying a resource the user 9 is interested in. For example, the personal information is entered by means of a data entry terminal at the point of presence 10 and transmitted through a communications line to the authentication server 4.

In exchange, the user 9 is handed in step P2 a computer-readable data carrier, for example a CD, a mini-disk, a chipcard or another suitable data storage module, which contains the serial number, for example in the form of a printed label, and location information for an entry point to the resource accessible through the communications network 5, for example an URL address (Uniform Resource Locator) of an entry page to the resource encoded as computer-readable data. The URL address is for example non-user-friendly represented by a string of many alphanumeric characters, e.g. http://72749/547etzjd4hb7dgdx/opeghfj633ore/9844378574rij", such that the location is unlikely to be traced by search engines and that the location information is difficult to be communicated to other users. Therefore, the CD preferably contains a computer program, from hereon called connection-

program, to direct the communication terminal 1 (or 3) to automatically connect to the location of the communications network 5 specified by the location information.

In step S1, upon reception of the personal user information, user identification information is assigned to the user, for example a user (or log-in) name and a secret user (or log-in) password. Furthermore, in step S1 the personal user information together with the user identification information is stored in the database 41 according to the diagram shown in Figure 2. According to Figure 2, the personal user information 7 is linked to the serial number 8. The personal user information 7 comprises the user identification information 71, including the user (or log-in) name 711 and the user (or log-in) password 712, the address (or phone number) 72 of the user's personal communication terminal, and possibly further personal user information 73.

In step A1 the user identification information 71, including the user name 711 and the user password 712, is communicated from the authentication server 4 to the user, for example by means of paper mail through the postal service or by means of e-mail or data messages transmitted to the personal communication terminal 2 or 3 identified by the address (or phone number) 72.

When the user wants to access the resource identified by the serial number 8, he uses his communication terminal 1 or 3 to connect to the entry point of the resource on the communications network 5, preferably by inserting the data carrier containing the connection-program into the communication terminal 1 or 3, respectively. In step U2, the serial number is transmitted by the communication terminal 1 or 3, respectively, over the communications network 5 to the authentication server 4, either automatically controlled by the connection-program or manually entered by the user upon request by the connection-program or the authentication server 4. Requests from the authentication server 4 are transmitted to the communication terminal 1 or 3, respectively, in a conventional way by means of software objects, for example HTML- (Hypertext Markup Language), XML- (Extended Markup Language) or

WML-objects (Wireless Markup Language) or executable programs such as Java-Applets (Java is a registered trademark of Sun Microsystems Inc.).

In step S2, the authentication server 4 compares the serial number received from the communication terminal 1 or 3, respectively, over the communications network 5 to the serial numbers 8 stored in the database 41. If the received serial number is validated as a legitimate serial number identifying a resource controlled by the authentication server 4, a request for entry of the user identification information is transmitted in step A2 by the authentication server 4 over the communications network 5 to the communication terminal 1 or 3, respectively.

In step U3, the user identification information, including the user name and the user password, entered by the user on his communication terminal 1 or 3, respectively, is transmitted over the communications network 5 to the authentication server 4.

In step S3, the authentication server 4 compares the user identification information received over the communications network 5 to the user identification information 71 stored in the database 41 and linked to the serial number 8 verified in step S2. If the received user identification information is validated, i.e. if it can be matched to user identification information linked to the serial number 8 validated in step S2, the authentication server 4 generates a challenge number. Verification of the user identity can also include verification of additional personal user information, such as name, mailing address or other personal information. The challenge number is a numeric or alphanumeric code, and is preferably generated by a random generator. The random generator is preferably implemented as a software program, but it could also be implemented as a hardware module. The challenge number is valid only for a one-time log-in during a limited time period, as will be described below.

In step A3, the challenge code generated in step S3 is transmitted by the authentication server 4 over the communications network 6 to the communication terminal 2 or 3, respectively, which is identified by the address (or phone number) 72 linked to the user identification information 71 verified in

step S3. Preferably, the challenge code is transmitted by means of special data messages, for example by means of SMS (Short Message Services) or USSD messages (Unstructured Services Data Element). To increase security, the challenge code can be transmitted in encrypted form.

In step S4, a timer is started by the authentication server 4. The timer is preferably a decrementing timer started with a pre-defined time value, for example a value of one minute or thirty seconds or even less. The timer is software controlled, and is based on the clock of the processor 43 of the authentication server 4 or based on a separate hardware clock.

The challenge code received from the authentication server 4 at the communication terminal 2 or 3, respectively, is either entered manually into the communication terminal 1 by the user upon request received from the authentication server 4 (not illustrated), or, in the optional step S6, it is automatically taken from the data message received from the authentication server 4 by a programmed relay module of the communication terminal 3, if the communication terminal 3 is used by the user to access both the communications networks 5 and 6.

In step U4, the challenge code received from the authentication server 4, is transmitted by the communication terminal 1 or 3, respectively, over the communications network 5 to the authentication server 4.

If the time value controlled by the timer has not been elapsed, i.e. if the elapsed time Δt does not exceed the time value set in step S4, the authentication server 4 compares in step S5 the challenge code received in step U4 to the challenge code transmitted in step A3. If the two codes coincide, the user is granted access to the resource identified by the serial number 8 in step A4. Preferably, at any given time, access to a resource identified by the serial number is granted only once to a particular user, thereby preventing that concurrent access to a resource is granted to more than one user identified by the same user identification information.

Industrial Applicability

The present invention can be used wherever user access to resources accessible over a communications network must be controlled, for example access to computer software objects such as computer programs, computer databases, computer data, computer directories or web pages, located on the Internet.

List of Reference Numerals

1	Communication terminal (personal computer)
2	Mobile communication terminal (mobile radio telephone)
3	Mobile communication terminal (personal data assistant with radio telephone module)
4	Authentication server
5	Communications network (Internet)
6	Communications network (mobile radio network)
7	Personal user information
8	Serial number
9	User
10	Point of presence
21, 31	Subscriber identification module (SIM-card)
41	Database
42	Data carrier
43	Processor
71	User identification information
72	Address of personal communication terminal (phone number)
73	Additional user information
711	User (log-in) name
712	User (log-in) password
A1	Communication of user identification information
A2	Request to enter user identification information
A3	Transmission of generated challenge code
A4	Granting user access to resource
P1	Transmission of personal user information
P2	Communication of serial number
S1	Recording of personal user information
S2	Verification of serial number
S3	Verification of user identification information, generating challenge code
S4	Starting timer
S5	Verification of returned challenge code
S6	Relaying of received challenge code
U1	Communication of personal user information

U2	Transmission of serial number
U3	Transmission of user identification information
U4	Transmission of received challenge code
Δt	Elapsed time

CLAIMS

1. Method for controlling access of a user to a resource accessible through a first communications network (5), the user accessing the first communications network (5) by means of a first communication terminal (1, 3), personal user information (7) including user identification information (71) being stored on an authentication server (4) connected to the first communications network (5), and user identification information, entered by the user on the first communication terminal (1, 3) and received at the authentication server (4) over the first communications network (5), being compared to the user identification information (71) stored on the authentication server (4), characterised

in that an address (72) of a second communication terminal (2, 3) is stored as part of the personal user information (7),

in that the authentication server (4) transmits a challenge code over a second communications network (6) to the second communication terminal (2, 3) identified by said address (72), after having validated the user identification information received from the first communication terminal (1, 3),

in that the challenge code received by the second communication terminal (2, 3) is transmitted by the first communication terminal (1, 3) over the first communications network (5) to the authentication server (4),

in that the authentication server (4) compares the challenge code received from the first communication terminal (1, 3) to the challenge code transmitted to the second communication terminal (2, 3), and

in that the authentication server (4) grants the user access to the resource after having validated the challenge code received from the first communication terminal (1, 3).

2. Method according to claim 1, characterised in that a timer is started by the authentication server (4) after the challenge code has been transmitted to the second communication terminal (2, 3), and in that the user is

denied access to the resource, if the challenge code is not received from the first communication terminal (1, 3) within a pre-defined time period.

3. Method according to one of the claims 1 or 2, characterised in that the personal user information (7) is linked to a serial number (8), the serial number (8) identifying the resource, and in that the user is requested to enter the serial number on the first communication terminal (1, 3) prior to the entry of the user identification information.

4. Method according to one of the claims 1 to 3, characterised in that the Internet is used as the first communications network (5), in that a mobile radio network is used as the second communications network (6), in that a mobile communication terminal is used as the second communication terminal (2, 3), in that the phone number assigned to the mobile communication terminal is used as the address, in that the challenge code is generated by means of a random generator, in that the challenge code is transmitted by the authentication server (4) over the mobile radio network to the mobile communication terminal, by means of data messages, and in that computer software objects are used as the resource.

5. Computerised authentication server (4) for controlling access of a user to a resource accessible through a first communications network (5), the authentication server (4) being connected to the first communications network (5), the authentication server (4) comprising a database (41) containing personal user information (7) including user identification information (71), the authentication server (4) comprising means to compare user identification information, entered by the user on a first communication terminal (1, 3) connected to the first communications network (5) and received at the authentication server (4) over the first communications network (5), to the user identification information (71) stored in the database (41), characterised

in that the personal user information (7) includes an address (72) of a second communication terminal (2, 3),

in that the authentication server (4) is connected to a second communications network (6) and comprises means for transmitting a challenge code over the second communications network (6) to the second communication terminal (2, 3) identified by said address (72), after having validated the user identification information received from the first communication terminal (1, 3),

in that the authentication server (4) comprises means for receiving a challenge code from the first communication terminal (1, 3) over the first communications network (5) and for comparing the challenge code received from the first communication terminal (1, 3) to the challenge code transmitted to the second communication terminal (2, 3), and

in that the authentication server (4) comprises means for granting the user of the first communication terminal (1, 3) access to the resource after having validated the challenge code received from the first communication terminal (1, 3).

6. Authentication server (4) according to claim 5, characterised in that it comprises a timer and means for starting the timer after the challenge code has been transmitted to the second communication terminal (2, 3) and for denying the user access to the resource, if the challenge code is not received from the first communication terminal (1, 3) within a pre-defined time period.

7. Authentication server (4) according to one of the claims 5 or 6, characterised in that the personal user information (7) is linked to a serial number (8), the serial number (8) identifying the resource, and in that the authentication server (4) comprises means for requesting the user to enter the serial number on the first communication terminal (1, 3) prior to the entry of the user identification information.

8. Authentication server (4) according to one of the claims 5 to 7, characterised in that the first communications network (5) comprises the Internet, in that the second communications network (6) comprises a mobile radio network, in that the address (72) is a phone number assigned to a mobile

communication terminal in the mobile radio network, in that the authentication server (4) comprises a random generator to generate the challenge code, in that the authentication server (4) comprises means to transmit the challenge code over the mobile radio network in data messages, and in that the resource comprises computer software objects.

9. Computer-readable data carrier (42), encoded with data representing a computer program, that makes it possible to direct a computerised server (4), connected to a first communications network (5) and comprising a database (41) containing personal user information (7) including user identification information (71), to compare user identification information, entered by the user on a first communication terminal (5) connected to the first communications network (5) and received at the authentication server (4) over the first communications network (5), to the user identification information stored in the database (41), characterised in that it further makes it possible to direct the computerised server (4)

to store an address (72) of a second communication terminal (2, 3) as part of the personal user information (7),

to transmit a challenge code over a second communications network, (6) connected to the computerised server (4), to the second communication terminal (2, 3), identified by said address (72), after having validated the user identification information received from the first communication terminal (1, 3),

to receive a challenge code from the first communication terminal (1, 3) over the first communications network (5) and to compare the challenge code received from the first communication terminal (1, 3) to the challenge code transmitted to the second communication terminal (2, 3), and

to grant the user of the first communication terminal (1, 3) access to the resource after having validated the challenge code received from the first communication terminal (1, 3).

10. Computer program product comprising: computer program code to direct a computerised server (4), connected to a first communications network (5) and comprising a database (41) containing personal user information (7) including user identification information (71), to compare user identification information, entered by the user on a first communication terminal (5) connected to the first communications network (5) and received at the authentication server (4) over the first communications network (5), to the user identification information stored in the database (41), characterised in that it further makes it possible to direct the computerised server (4)

to store an address (72) of a second communication terminal (2, 3) as part of the personal user information (7),

to transmit a challenge code over a second communications network, (6) connected to the computerised server (4), to the second communication terminal (2, 3), identified by said address (72), after having validated the user identification information received from the first communication terminal (1, 3),

to receive a challenge code from the first communication terminal (1, 3) over the first communications network (5) and to compare the challenge code received from the first communication terminal (1, 3) to the challenge code transmitted to the second communication terminal (2, 3), and

to grant the user of the first communication terminal (1, 3) access to the resource after having validated the challenge code received from the first communication terminal (1, 3).

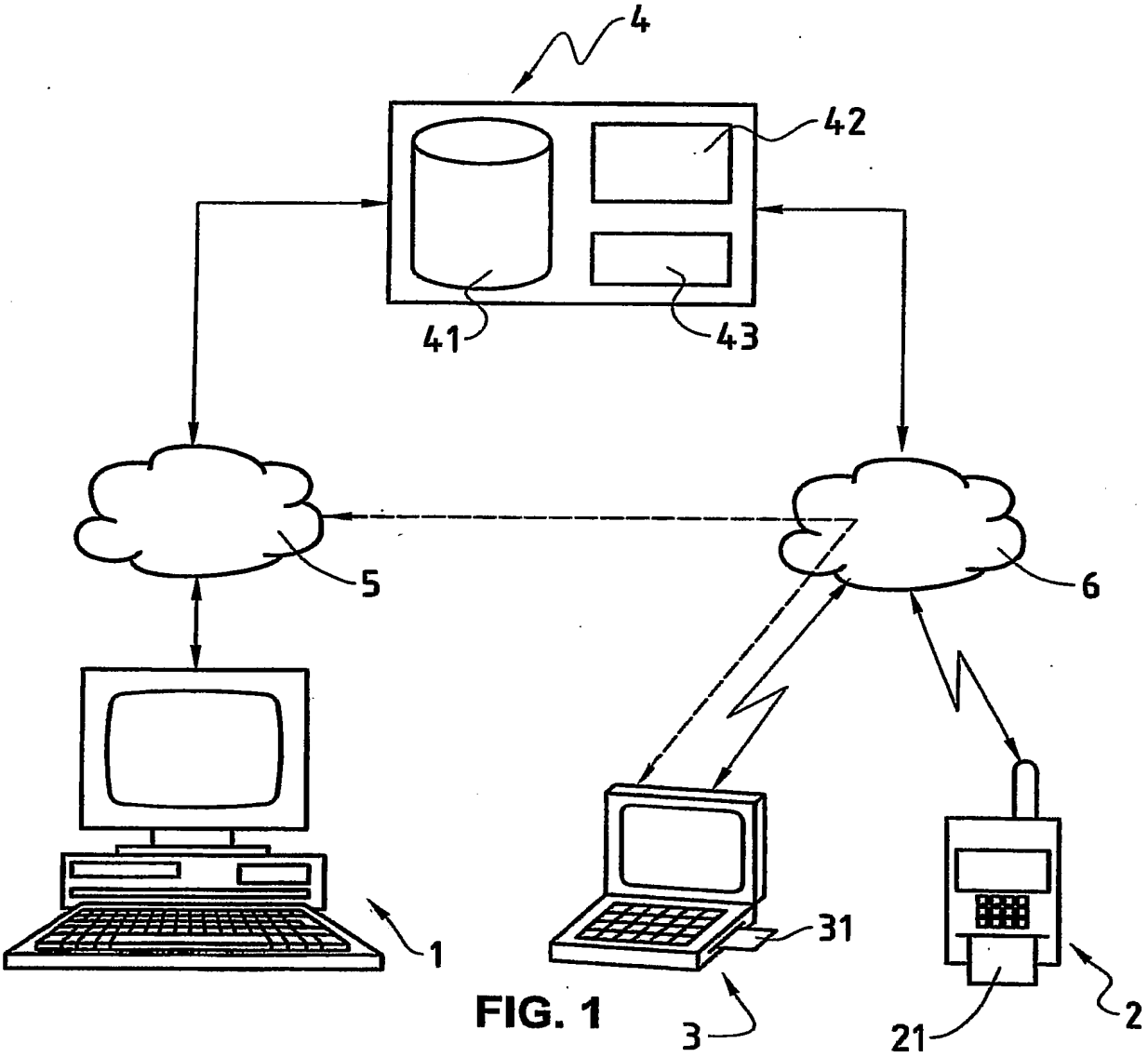


FIG. 1

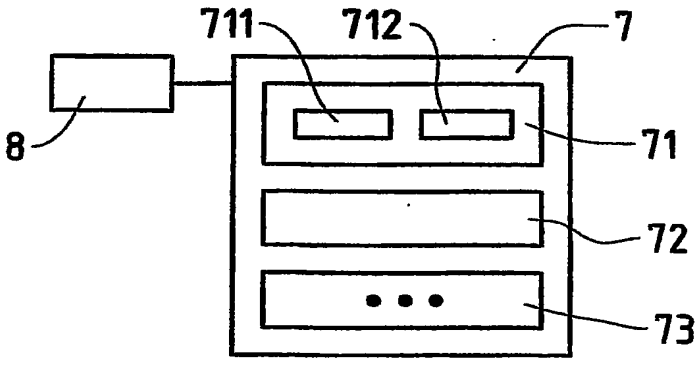


FIG. 2

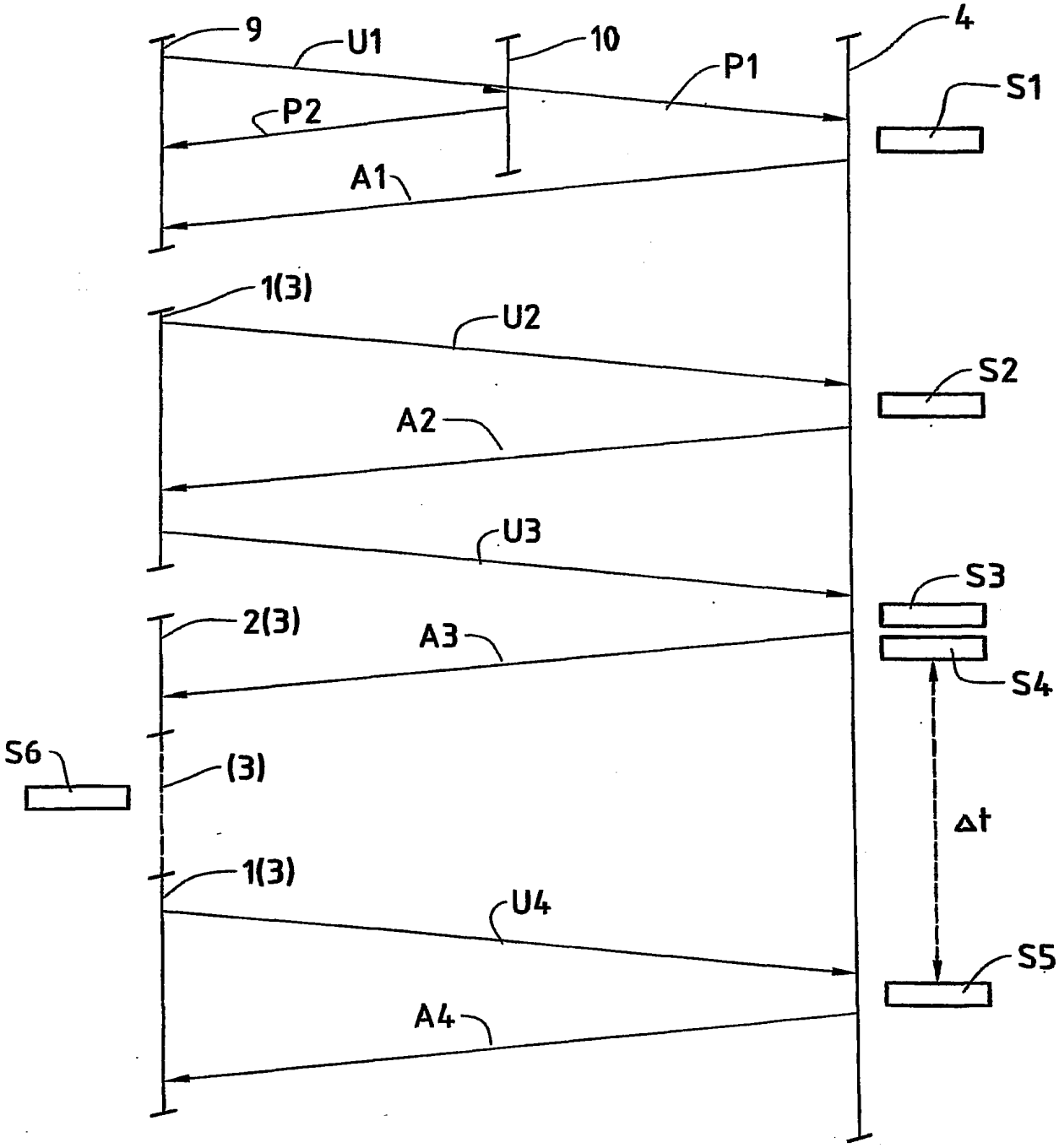


FIG. 3

INTERNATIONAL SEARCH REPORT

In tional Application No
PCT/CH 02/00050

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 844 551 A (VENEKLASE BRIAN J) 27 May 1998 (1998-05-27) abstract column 6, line 5 -column 7, line 10 column 8, line 28 -column 9, line 18	1,2,4-6, 8-10
Y	---	3,7
X	US 6 078 908 A (SCHMITZ KIM) 20 June 2000 (2000-06-20) abstract column 6, line 55 -column 7, line 24 column 8, line 11-65 claims 10,11	1,2,4-6, 8-10
Y	---	3,7
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 December 2002	11/12/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Ruiz Sanchez, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/CH 02/00050

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 01 80525 A (SUN MICROSYSTEMS INC) 25 October 2001 (2001-10-25) abstract page 3, line 34 -page 4, line 10 page 5, line 6-29 page 6, line 19-34	3,7
Y	US 6 067 623 A (BLAKLEY III GEORGE ROBERT ET AL) 23 May 2000 (2000-05-23) abstract column 3, line 9-23 column 4, line 50-64 column 5, line 22-30	3,7

INTERNATIONAL SEARCH REPORT

Information on patent family members

In tional Application No
PCT/CH 02/00050

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0844551 A	27-05-1998	US 5881226 A	09-03-1999
		EP 0844551 A2	27-05-1998
US 6078908 A	20-06-2000	DE 19718103 A1	04-06-1998
		AT 226346 T	15-11-2002
		AU 6354598 A	05-11-1998
		BR 9801177 A	20-03-2001
		CN 1207533 A	10-02-1999
		DE 59805939 D1	21-11-2002
		EP 0875871 A2	04-11-1998
		JP 10341224 A	22-12-1998
		TW 425804 B	11-03-2001
WO 0180525 A	25-10-2001	AU 4529201 A	30-10-2001
		WO 0180525 A1	25-10-2001
US 6067623 A	23-05-2000	NONE	